

INTERNATIONAL PRELIMINARY EXAMINATION REPORT
International Application No. PCT/DE 03/01998

I. Basis of the report

With regard to **components** of the international Application

this report has been drawn on the basis of (Substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments. Rules 70.16 and 70.17):

The description, pages:

2-6 original version

1, 1a received 08/04/2004, with letter dated 08/03/2004

The claims, Nos.:

1-10 received 08/04/2004, with letter dated 08/03/2004

The drawings, sheets/fig.:

1/1 original version

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Yes: Claims	1-10
	No: Claims	

International Application No. PCT/DE 03/01998

Industrial Applicability (IA)	Yes: Claims	1-10
	No: Claims	

see appended sheet

INTERNATIONAL PRELIMINARY EXAMINATION REPORT - UNPENDED SHEET
International Application No. PCT/DE 03/01998

Re Section V:

1. The subject matter of the present Application relates to a method for making available security in the transmission of data from and to a subscriber terminal unit of a mobile communications network and to a device for making available of such security functions, according to the features of the generic part of newly filed Claim 1 and independent Claim 8.
2. The most proximate related art is represented by document WO-A-01 33889 (first document cited in the International Search Report) and is acknowledged in the introductory part of the specification.
3. According to the features of the two independent Claims 1 and 8, that which is essential to the present invention, is that in one direction for making available security functions in the network nodes of a mobile communications network, a real-time analysis of the data flow from and to the subscriber terminal unit is carried out, data having contents previously specified by the subscriber or the network operator being recognized and processed further, but first an authentication method is carried out by which the subscriber authenticates himself vis-à-vis the device.

The concept on which this is based is also not described or made obvious by the remaining documents that have

become known, thereby the changed independent claims satisfy the requirements of Article 33 PCT.

4. The dependent claims refer to an advantageous embodiment of the subject matter of the respective independent claim. They only restrict the claimed protective range of the corresponding independent claim, and therefore also satisfy the requirements of Article 33 PCT.

The present invention relates to a method and a device for making available security functions during the transmission of data from or to a subscriber terminal unit of a mobile communications network.

5 Current and new data services offer subscribers of mobile communications networks direct access to the Internet and other public data networks. Therefore, the mobile telephone used for mobile application, and ancillary equipment driven by it, such as a notebook or a personal digital assistant, are at
10 the mercy of the most varied attacks by third parties, similar to what happens in a fixed network-based Internet access.

WO 01 3389 A1 describes a method for making available security functions during the transmission of data from or to a subscriber terminal unit of a mobile communications network, a
15 real-time analysis of the data flow from and to the subscriber terminal unit being carried out in a device of a network node of the mobile communications network; and data having contents specified previously by the subscriber or a network operator/provider being recognized and processed further. A
20 subscriber-individual making available of security functions is evidently not assured in this case.

WO 00 36793 relates to a method for filtering packet data in GPRS connections, in order to establish and to influence the so-called "quality of service" of a packet data connection.
25 The purpose of this access device is less a protection from undesired and malicious data than a speeding up of the data transmission or a best possible utilization of the available capacities in the communications network.

It is the object of the present invention to state a method
30 and a device for making available security functions in the

transmission of data from and to a subscriber terminal unit of a mobile communications net, so as to effectively protect the subscriber terminal unit and units connected to it or combined with it.

- 5 This object is attained by the features of the independent claims.

The crux of the present invention is, in a cellular mobile telephony network, to offer a security service that is able to be personalized, individually by cellular mobile telephony connection and subscriber.

10

What Is Claimed Is

1. A method for making available security functions for the transmission of data from and to a subscriber terminal unit of a mobile communications network, a real-time analysis of the data flow (12) from and to the subscriber terminal unit (13) being carried out in a device (1) of a network node of the mobile communications network (10), data having contents specified previously by the subscriber or a network operator/provider being recognized and processed further, wherein first an authentication method is carried out by which the subscriber authenticates himself vis-à-vis the device (1).
2. The method as recited in Claim 1, wherein the data traffic from and to specified senders and receivers is recognized and processed further.
3. The method as recited in one of the preceding claims, wherein the recognized data are selected and/or isolated and/or deleted and/or made available to the subscriber or the network operator/provider separately for further processing.
4. The method as recited in one of the preceding claims, wherein a filtering particularly of the IP/TCP-based data traffic is carried out.
5. The method as recited in one of the preceding claims, wherein the arising data transfer volume is limited to a measure established by the subscriber or the network operator.
6. The method as recited in one of the preceding claims, wherein the arising data transfer costs are limited to a

measure established by the subscriber or network operator.

7. The method as recited in one of the preceding claims, wherein the subscriber, network operator or provider is notified upon the recognition of certain data contents and/or senders.
8. A device for making available security functions for the transmission of data from and to a subscriber terminal unit of a mobile communications network, including a security and filtering device (1) having the following components:
 - a filter component (2) for the real-time analysis of the data flow from and to the subscriber terminal unit;
 - an authentication component (3) for authenticating the subscriber vis-à-vis the security and filtering device;
 - an administrative component (4) as the interface to the subscriber;
 - a database (5) for storing subscriber-specific and network operator-specific data as well as security and filtering functions.
9. The device as recited in Claim 8, wherein the security and filtering component (2) is positioned in one or more network nodes of the mobile communications network (10).
10. The device as recited in Claim 8 or 9, wherein for certain data contents, special filter components are established.